



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/629,292	07/29/2003	Mihai Christodorescu	1512.149	6450
72088 7590 04/04/2008 WISCONSIN ALUMNI RESEARCH FOUNDATION C/O BOYLE FREDRICKSON S.C 840 North Plankinton Avenue Milwaukee, WI 53203				
			EXAMINER	
			GELAGAY, SHEWAYE	
		ART UNIT	PAPER NUMBER	
		2137		
		NOTIFICATION DATE	DELIVERY MODE	
		04/04/2008	ELECTRONIC	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@boylefred.com

**Office Action Summary****Application No.**

10/629,292

**Applicant(s)**

CHRISTODORESCU ET AL.

**Examiner**

SHEWAYE GELAGAY

**Art Unit**

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 27 December 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-946)
- 3) ☐ Information Disclosure Statement(s) (PTO/SG/US)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on December 27, 2007. Claim 1 has been amended. Claims 1-17 are pending.

### *Response to Arguments*

2. Applicant's arguments with December 27, 2007 have been considered but are moot in view of the new ground(s) of rejection.

### *Specification*

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The term "computer readable storage medium" lacks antecedent basis in the specification.

### *4. Claim Rejections - 35 USC § 101*

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-17 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 1 is directed to a computer program stored on a computer readable storage medium in which the "computer readable storage medium" is not defined in the specification. The context the medium was used in the claim would fairly suggest to one ordinary skill signals or other forms of propagation and transmission media, typewritten or handwritten

Art Unit: 2137

text on paper, or other items failing to be an appropriate manufacture under 35 USC 101 in the context of computer-related inventions.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1-3 and 6-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg U.S. Patent Number 6,357,008 in view of Christodorescu "Detecting Malicious Patterns in Executables via Model Checking" University of Wisconsin, July 12, 2002, page 1-15. As per claim 1:

Nachenberg teaches a computer program for identifying malicious portions in a suspect computer program comprising:

a preprocessor portion for receiving the suspect computer program and creating a logically equivalent standardized version of the suspect program; (col. 5, lines 27-39; col. 6, line 53-col. 7, line 22)

a library of standardized malicious code portions; (col. 7, line 23-col. 8, line 31; col. 9, lines 26-65) and

a detector portion reviewing the standardized version against the library of malicious code portions to provide an output indicating when a malicious code portion is present in the suspect program. (col. 9, line 66-col. 10, line 10; col. 15, line 38-col. Col. 16, line 63)

Nachenberg does not explicitly disclose creating a logically equivalent standardized version of the suspect program without executing the suspect program. Christodorescu discloses creating a logically equivalent standardized version of the suspect program without executing the suspect program. (page 12-24) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Nachenberg with Christodorescu in order to analyze the program semantic structure to check the presence of malicious properties. (page 12, Christodorescu)

As per claim 2:

The combination of Nachenberg and Christodorescu teaches all the subject matter as discussed above. In addition, Nachenberg further teaches wherein the standardized version identifies the execution order of instructions of the suspect program and wherein the detector portion reviews the instructions of the standardized version according to the execution order. (col. 2, line 38-col. 4, line 65; col. 7, line 23-col. 8, line 31; col. 9, line 26- col. 10, line 10; col. 15, line 38-col. 16, line 63)

As per claim 3:

The combination of Nachenberg and Christodorescu teaches all the subject matter as discussed above. In addition, Nachenberg teaches wherein the preprocessor identifies the execution order of the instructions by generation of a control-flow listing of the instructions. (col. 2, line 38-col. 4, line 65; col. 9, lines 26-67)

As per claim 6:

The combination of Nachenberg and Christodorescu teaches all the subject matter as discussed above. In addition, Nachenberg further teaches wherein the standardized version

Art Unit: 2137

removes irrelevant portions of the suspect program. (col. 13, line 42-col. 15, line 37)

As per claim 7:

The combination of Nachenberg and Christodorescu teaches all the subject matter as discussed above. In addition, Nachenberg teaches wherein the preprocessor removes irrelevant portions by identifying irrelevant portions to the detector so that the detector ignores identified irrelevant portions when reviewing the standardized version. (col. 13, line 42-col. 15, line 37)

As per claim 8:

The combination of Nachenberg and Christodorescu teaches all the subject matter as discussed above. In addition, Nachenberg teaches wherein the irrelevant portions are one or more nop instructions. (col. 13, line 42-col. 15, line 37)

As per claim 9:

The combination of Nachenberg and Christodorescu teaches all the subject matter as discussed above. In addition, Nachenberg teaches wherein the standardized version uses uninterpreted variables. (col. 13, line 42-col. 15, line 37)

As per claim 10:

The combination of Nachenberg and Christodorescu teaches all the subject matter as discussed above. In addition, Nachenberg teaches wherein the suspect program is a binary executable and wherein the preprocessor receives the binary executable to generate a listing of instructions and data values. (col. 13, line 42-col. 15, line 37)

2. Claims 4-5 and 11-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg U.S. Patent Number 6,357,008 in view of Christodorescu "Detecting Malicious

Art Unit: 2137

Patterns in Executables via Model Checking” University of Wisconsin, July 12, 2002, page 1-29 in view of Ho et al. (hereinafter Ho) U.S. Patent Number 7,188,369.

As per claims 4 and 14:

The combination of Nachenberg and Christodorescu teaches all the subject matter as discussed above. Both references do not explicitly disclose wherein the standardized version maps instructions of the suspect program to corresponding standard synonym instructions. Ho in analogous art, however, discloses wherein the standardized version maps instructions of the suspect program to corresponding standard synonym instructions. (col. 5, lines 25-col. 6, line 40) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Nachenberg and Christodorescu with Ho in order to receive external instructions and for execution and perform their respective antivirus functionalities. (col. 6, lines 18-21; Ho)

As per claims 5 and 15:

The combination of Nachenberg, Christodorescu and Ho teaches all the subject matter as discussed above. In addition, Ho further teaches wherein the standard synonym instructions are different in number from the instructions of the suspect program to which the synonym instructions map. (col. 5, lines 25-col. 6, line 40)

As per claims 11 and 16:

The combination of Nachenberg and Christodorescu teaches all the subject matter as discussed above. Both references do not explicitly disclose including a library of patterns matching to one or more instructions of the suspect program and wherein the preprocessor creates the standardized version by replacing instructions of the suspect program with matching

Art Unit: 2137

ones of the library of patterns and wherein the library of standardized malicious code portions are also collections of ones of the library of patterns. (col. 5, lines 25-col. 6, line 40) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Nachenberg with Ho in order to receive external instructions and for execution and perform their respective antivirus functionalities. (col. 6, lines 18-21; Ho) As per claims 12 and 17:

The combination of Nachenberg, Christodorescu and Ho teaches all the subject matter as discussed above. In addition, Ho further teaches wherein a pattern is at least one instruction logically replacing at least one different instruction in the suspect program. (col. 5, lines 25-col. 6, line 40)

As per claim 13:

The combination of Nachenberg, Christodorescu and Ho teaches all the subject matter as discussed above. In addition, Ho further teaches wherein a pattern in a tag replacing at least one instruction logically having no substantive effect on the execution of the suspect program; a library of patterns is implemented as a look-up table matching instructions to the patterns. (col. 5, lines 25-col. 6, line 40)

### *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).



A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEWAYE GELAGAY whose telephone number is (571)272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Art Unit: 2137

/S. G./

Examiner, Art Unit 2137

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137